サイバーレジリエンスを通じた セキュリティと コンプライアンス態勢の強化

セキュリティとコンプライアンス態勢を強化するための
サイバーレジリエンスの重要性について、
最新の視点から解説

ABSOLUTE®

コンプライアンスとは

包括的で効果的なリスクベースのコンプライアンス戦略の意味を理解することが、その実現への第一歩となります。「コンプライアンス」の定義は、長年にわたり、データプライバシー、データ保護、サイバーセキュリティなどの用語と大きく混同されてきました。これらの用語は類似しており、相互に関連していますが、これらの用語の違いと関連性の両方を正しく理解することが極めて重要です。

データプライバシーは、どのような種類のデータ(通常、組織によって収集、処理、または転送されるもの) が機密情報とみなされるかを規定する法的概念です。データプライバシーは、現在、一般的に個人が持つ権利とみなされています。したがって、組織は、機密情報や個人を特定できる情報を保護するために、どのような保護措置を講じなければならないかを理解することが非常に重要です。

サイバーセキュリティは、米国 CISA (サイバーセキュリティ・インフラストラクチャ・セキュリティ局) によって「ネットワーク、デバイス、データを不正アクセスや犯罪利用から保護する技術、情報の機密性、完全性、可用性を確保する実践」と定義されています [1]。この広い用語には、データ保護とデータプライバシーの両方が含まれています。データ保護を通じて個人のデータプライバシーを確保することは、サイバーセキュリティの広義の定義に該当します。

データ保護は、機密データ (データプライバシーで定義) を確実に保護するために取られるすべての措置を含みます。この用語は、組織が扱う個人を特定できる情報 (PII) をあらゆるレベルで保護するための具体的な技術的ソリューションを示すためによく使われます。

コンプライアンスとは、簡単に言えば「規則に従うこと」です。組織や統治機関によって作成されるコンプライアンスポリシー (または一連の規則) は、通常、データ保護やデータプライバシーを実現するために実施されるものです。これらの規則は、組織が維持しなければならない「最低限許容できる」状態の概要を示しています。組織が一定のセキュリティ態勢を維持し、潜在的な侵害やデータ漏えいのリスクを排除することを確実にします。

リスクベース・コンプライアンスを適用してセキュリティを確保

コンプライアンスとコンプライアンス対策は、データのプライバシーと保護を確保する組織の能力を強化し、確保するための機能として存在します。コンプライアンス基準は、組織が潜在的なリスクを把握し、サイバー攻撃や潜在的なデータ侵害を防止するための強固なセキュリティ構造を構築するために設けられています。

コンプライアンスを考えるとき、次に考えるのはセキュリティであるはずです。この 2 つはたがいに関連し合っています。強力なサイバーセキュリティ体制 (およびセキュリティ管理体制) がなければ、業界のコンプライアンス規制を順守することはまず不可能です。同様に、コンプライアンスについて考えなければ、セキュリティ戦略も不十分なものになるでしょう。

では、リスクベースのコンプライアンス戦略の構築はどのように始めればよいのでしょうか。従来の「チェックボックスで確認」する態勢は、もはや通用しないのです。

潜在的な「攻撃対象」を検討

何よりもまず、多くの組織が陥りがちな「自分には関係ない」「気にする必要はない」という考え方に陥らないことが重要です。現代では、ほとんどすべての組織が何らかの形で機密データを処理、保管、共有しています。

PII (Personally Identifiable Information) とは、個人を特定できる情報のことで、さまざまなデータが含まれます。個人の氏名、住所、電話番号など、あらゆるものが含まれます。クレジットカード番号のような機密性の高い情報である必要はありません。組織としてこのようなデータを収集している場合、そのデータの安全性を確保する責任があります。

顧客情報の保管を外部に委託していれば自組織に責任はないのでしょうか？そうではありません。顧客データをデータベースから第三者のサービスに転送することも、組織の責任です。

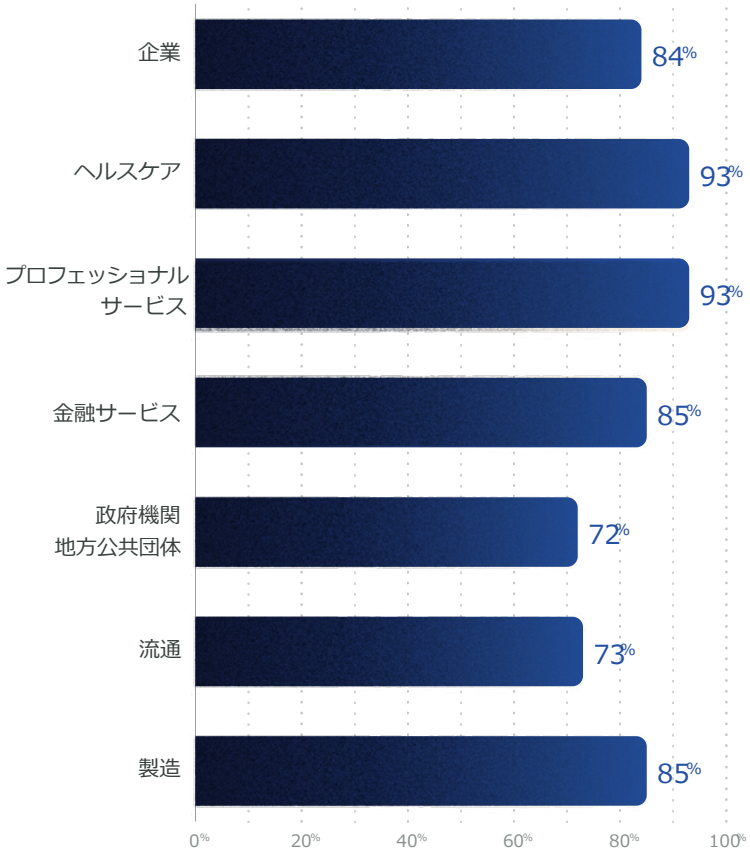
しかし、今日の多くの組織では、特にエンドユーザー・デバイスのデータ保護に万全を期しているとは言えません。このことは、Absolute で健全なデータの暗号化の状況を確認すれば、明らかです。

暗号化は、ネットワーク上で送信されるトラフィックの安全性を確保するための基本的なセキュリティ対策です。万が一、トラフィックが傍受された場合でも、暗号化によって暗号化解除や漏洩を防止することができます。世界中の Absolute 対応デバイスから収集したデータによると、暗号化のパフォーマンスは業種によって 大きく異なっています。プロフェッショナルサービス業のデバイスは、最も高い暗号化健全率を誇り、93% という値を示していますが、政府機関のデバイスは最も低く、72% という暗号化率を示しています (図 1.1 参照)。これらの指標から、かなりの割合のデバイスが暗号化されないまま放置され、攻撃に対して脆弱な状態になっていることがわかります。

図 1.1

暗号化

業界別健全なデバイスの比率



2023 年 1 月 9 日時点のデータ。30 日間有効なデバイスの数。エンタープライズ – 4,300 デバイス、ヘルスケア – 1,200 デバイス、プロフェッショナルサービス - 68 万デバイス、金融サービス - 56 万デバイス、リテール - 22 万デバイス、製造業 - 13 万デバイス

まずは、組織が収集しているデータを特定することが重要です。データは、組織の中に仮想的に入ってから最終的に廃棄されるまでの間、どのように処理されるのでしょうか。ネットワーク、ストレージ、Web フォームなど、あらゆるデータをマッピングして、見落としがないようにしましょう。このプロセスにより、組織の潜在的な攻撃対象領域を明確に把握することができます。Gartner は、「2023 年までに、世界人口の 65% が最新のプライバシー規制の下で個人データを保護されるようになる」と言っています。また、「COVID-19 が世界的に流行した際、コストの最適化に注力した組織もあったが、急速に進化するプライバシー環境の要求をビジネスのデータ戦略に組み込むことが最も重要である」[2] と強調しています。データの流れを描き出すことにより、組織のあらゆるレベルで、最も効率的にデータの保護に取り組むための可視性を得ることができます。

リモートワークにおける本質的なリスク

組織内でどのようなデータがどこに流れているかを考える一方で、リモートワークやモバイルワークの増加によって攻撃対象が本質的に拡大している可能性があることを念頭に置く必要があります。もはやエンドポイントは、「オフィスネットワーク」という保護された領域内に安全に保管されているわけではないのです。

組織ネットワークへの接続は、1 日平均で約 4 カ所から行われており、12 月のホリデーシーズン前後には若干減少しています (図 1.2 参照)。リモートワークが普及したからといって組織ネットワークへの接続接続がなくなったわけではありません。

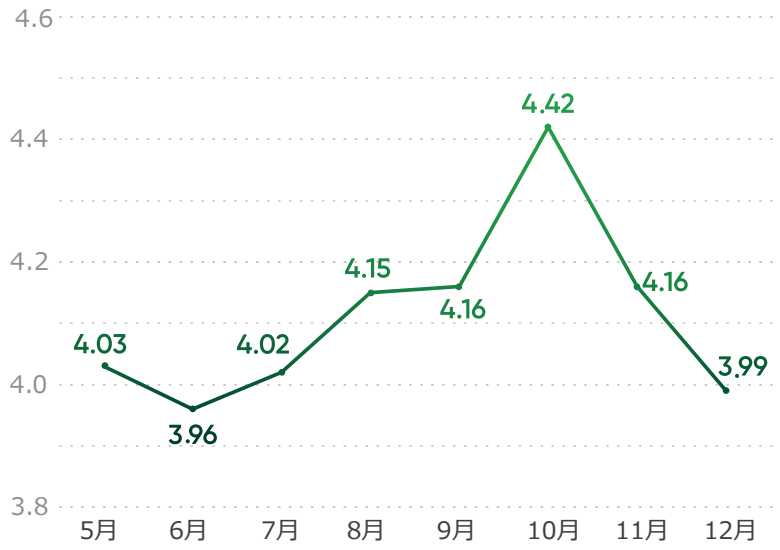
従業員が自分のデバイスからアクセスするデータは、傍受の影響をはるかに受けやすいものです。安全でないネットワークや悪質な業者が横行しており、特に従業員がリモートワークを行っている場合、それを避けることは困難です。

従業員は仕事を効率的に進めるために、様々な外出先からも機密データにアクセスします。実際、Absolute のデータによると、2022 年には組織向けデバイスの 76% に機密データが含まれていることが判明しています。この割合は、2021 年の 75% からわずかに上昇し、依然として高い水準にあります。

業種別を詳しく見てみると、意外にも、機密データを保管しているエンドポイントの割合が最も高いのは金融サービス業です (デバイスの 85%)。ヘルスケアでの影響は最も低い値を示していますが、それでも 50% を大きく超えており、エンドポイントの 69% が機密データを保存しています (次ページの図 1.3 を参照)。この機密データは、エンドポイント自体に保存されています。したがって、デバイスを監視するための適切な可視性とセキュリティ管理がなければ、知らないうちにデータが流出し、組織のコンプライアンス態勢が損なわれる可能性があります。

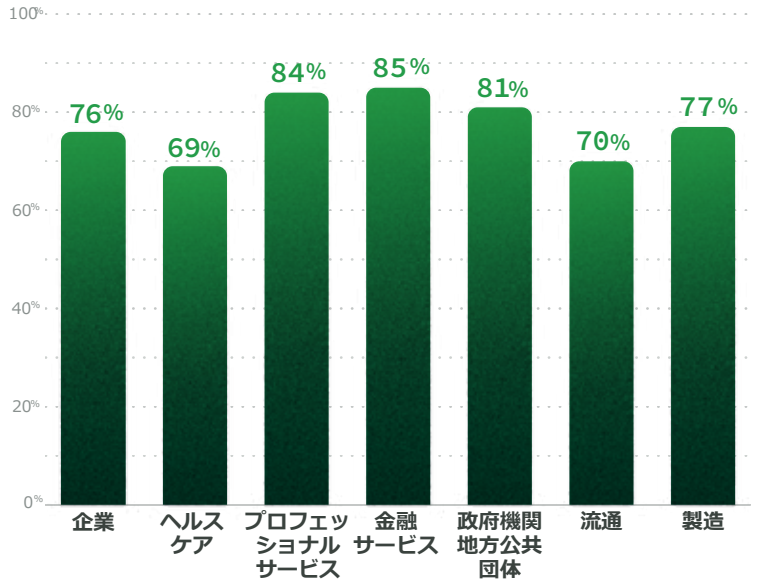
リモートワークにおける本質的なリスク

図 1.2
企業向けデバイスが 1 日あたりに使用される平均ロケーション数
8 カ月間



2022 年 5 月から 12 月までの 270 万台のジオロケーションデータが存在するエンタープライズ端末に基づく分析。ジオロケーションの手法には、Wi-Fi による測位 / 三角測量、GPS、Windows のロケーション API、Google のジオロケーション API (優先順位順) が含まれる。

図 1.3
機密情報を含むデバイスの比率
業種別



2023 年 1 月 6 日までの 1 週間のデータ。機密データを持つデバイスの数。企業：55 万 6,000 台 (72 万 9,000 台中)、ヘルスケア:19 万 5,000 台 (28 万 1,000 台中)、プロフェッショナルサービス：2 万 9,000 台 (3 万 5,000 台中)、金融サービス：7 万台 (8 万 2,000 台中)、政府：11 万 4,000 台 (14 万台中)、小売:2 万 1,000 台 (3 万台中)、製造:1 万 1,000 台 (1 万 5,000 台中)。

順守すべき法律やルール

コンプライアンスについては、フォローしたり守ったりしやすいものばかりではありません。世界中で 900 以上の監督機関が、毎日平均 200 以上の規制の更新を発行しています。このことが、多くの組織がコンプライアンスを無視したい (あるいはあまり注意を払いたくない) と考える主な理由となっています。

しかし、無視することが逃げ道というわけにはいきません。「提案」レベルの規定もありますが、法律として規定されているものもあります。規制を守らなければ、組織は深刻な財政的影響を受けることになります。

一般に、コンプライアンスには 3 つの柱があると言われています。

1. 法律、政令、規則などの形で、従わなければならない法規制。例えば、医療業界では HIPAA や HITECH、公共分野では FISMA や IRS Publication 1075、商業分野では Sarbanes Oxley Act、最後に個人情報保護法、GDPR やカリフォルニア消費者保護法などのプライバシーに関する法律が挙げられる。
2. シンガポール MAS や NERC のような業界標準機関から、従うべき一般的な勧告。場合によっては、PCI-DSS のような強制措置まで用意されていることもある。多くの場合、提供されるガイダンスはより規範的で、組織が準拠するだけでなく、より重要なセキュリティ態勢を強化するために適用すべき特定の管理方法を明確に示している。
3. ISO、NIST、CJIS のような業界標準。あくまで推奨であり、対応すべき義務があるものではない。

どのような規制や業界標準が自分の組織に適用されるかは、会社、業界、場所など多くの事柄に左右されます。また、コンプライアンスを維持することは、規制が常に更新されているため、最新の情報を入手することを意味します。Thomson Reuters のような企業は、顧客が規制の更新を遅れないようにするための専用サービスを提供していますが、これらのサービスは高価です。ほとんどの場合、規制や更新を常に把握することは、組織内のチームに委ねられています。

コンプライアンス違反のコスト

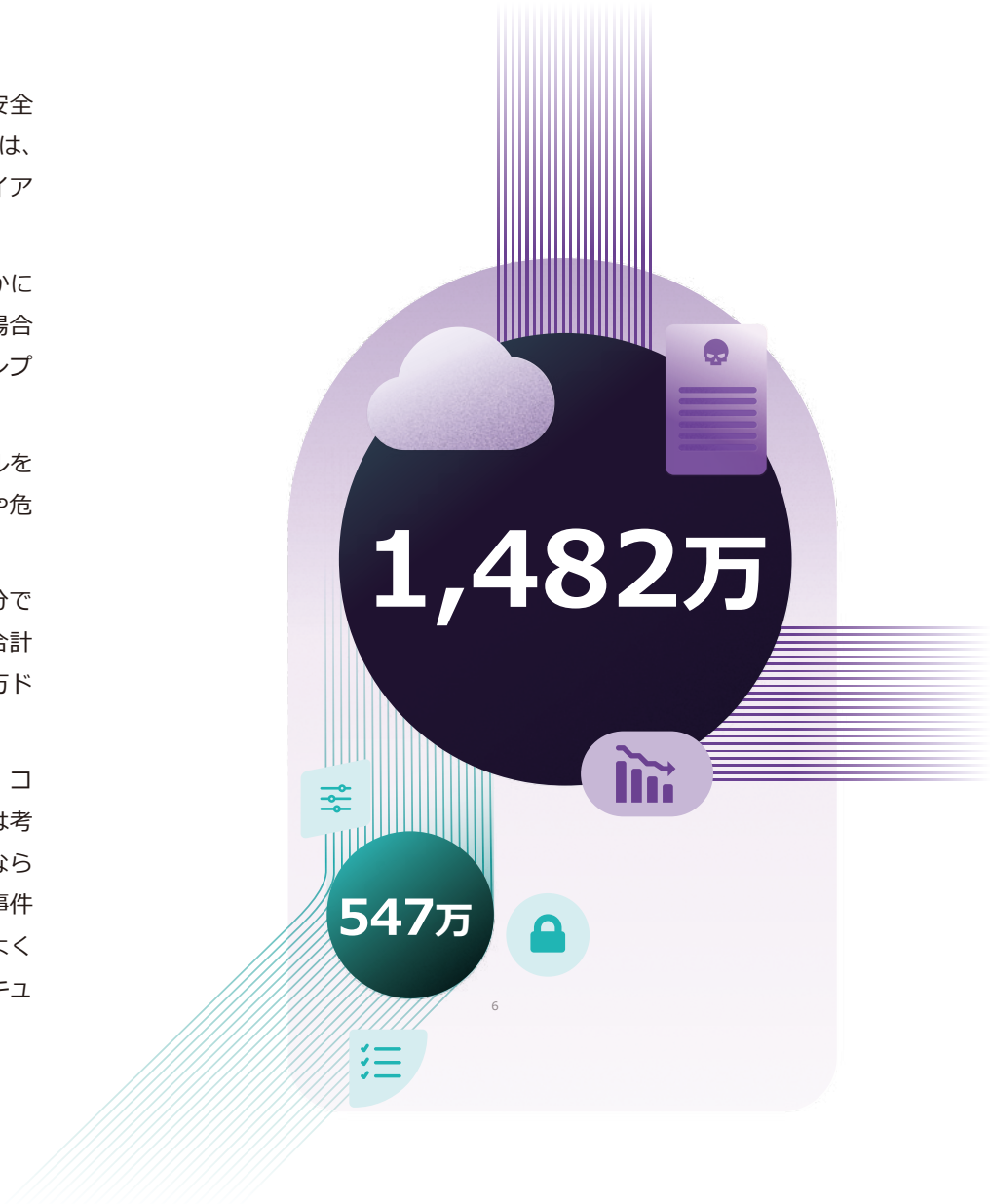
上述のように、多くの組織はできるだけ低コストで簡単に、政府やその他の団体がデータの安全性を確保し、多くの規制を順守したいと考えていますが、コンプライアンスを確保することは、時間がかかり、困難で、費用のかかるプロセスであるのが現実です。その努力は、コンプライアンス違反の潜在的コストに見合うものなのでしょうか。

データによると、こうした努力を行うことは、コンプライアンス違反が発覚するよりもはるかにコストが低いことが分かっています。Ponemon の調査によると、組織が規制を順守しない場合のコストは、2.7 倍になります。コンプライアンスにかかる平均コストは 547 万ドルで、コンプライアンス違反の平均コストは 1,482 万ドル、その差は年間 935 万ドルです[3]。

Forrester によると、企業は情報漏えいの発見と復旧に中央値で 37 日、平均値で 240 万ドルを費やしています。世界的に見ると、敵の発見と攻撃の根絶に平均値で 27 日、インシデントや危機対応の準備が十分でない組織では平均値で 35 日かかっています。

侵害からの復旧に要した日数は、平均値で 10 日、インシデントおよび危機対応の準備が十分でなかった組織では平均値で 11 日でした。また、侵害 1 件あたりのコストは、世界平均で合計 240 万ドルでしたが、インシデントや危機対応の準備が十分でなかった組織では、平均 300 万ドルとなっています[4]。

この分析では、罰金など、コンプライアンス違反による測定可能なコストを考慮しています。コンプライアンスの欠如によって発生したデータ漏洩やサイバー攻撃による長期的な風評被害は考慮されていません。注目すべきは、コンプライアンス違反のコストが、組織が耐えなければならないものにとどまらず、「個人的」なものになり始めていることです。Equifax のデータ流出事件のように、大手上場企業の CEO が壊滅的なデータ流出事件を受けて退陣を迫られるケースはよくありますが、Gartner は、「2026 年までに、C レベル経営者の少なくとも 50% が、サイバーセキュリティリスクに関する業績要件を雇用契約に盛り込むことになる」[5] と予測しています。



ケーススタディ：マリオット・インターナショナル

マリオット・インターナショナル (スターウッド) は 2018年 9月に大規模なデータ流出を起こし、5億人の顧客のPII (氏名、住所、パスポート番号、一部のクレジットカード情報)が流出しました[6] 。最終的に、英国のデータ管理機関である情報コミッショナーオフィス (ICO) [7] に命じられ 1,840万ポンドの罰金を支払うとともに、流出の原因とされた「スターウッドシステム」プラットフォームの段階的廃止を強いられました。マリオットは現在も営業を続けていますが、このデータ流出事件で評判が落ちたことには間違いありません。

マリオットは、データ流出とそれに伴うコストに見舞われた多くの大手企業のうちのひとつに過ぎません。他の組織も注意し、どの企業も免責されないことを理解する必要があります。あなたの組織のデータが安全でないなら、おそらく危険にさらされるでしょう。リスクベースのコンプライアンス戦略を積極的に検討し、情報漏えいを防ぐためにセキュリティ体制を可能な限り強固にすることが重要です。

リスクベース・コンプライアンスによるセキュリティの確保

以上、コンプライアンスの定義と適用について述べました。次は、組織としてコンプライアンスを確保する方法について説明します。コンプライアンスを維持し、セキュリティを強化するために、さまざまな法律、規制、命令、業界の勧告に対応するためにできることは数多くあります。

1. 法規制の把握とデータの理解

コンプライアンスを実現するための最初のステップは、コンプライアンスに準拠する必要があるものを理解することです。地域、業種、規模、収集するデータの種類によって、適用される規制は異なります。まずは適用される規制と業界標準を理解することです。

適用される規制と業界標準を理解したら、次のステップはデータを管理することです。組織内のデータの保存、転送、共有の場所を地図上にまとめることは、あらゆる場所、あらゆる接続においてデータを確実に保護するために不可欠な最初のステップです。また、データを分類し、収集したデータを機密性のレベルごとにグループ化することも有効です。これは、どのデータ（および場所）に特別な注意が必要かを特定し、保護策を講じる際に役立ちます。

2. 役に立つリソースとソリューションの発見

どのようなデータをどこで保護する必要があるのかを理解したら、次はそのデータを（保存時と転送時の両方で）ロックする方法を考えなければなりません。簡単なことのように聞こえますが、その方法を決定するのは容易なことではありません。組織内でできることと、アウトソーシングすべきことは何かを Google で検索すると、何十万もの企業がヒットしますが、いずれも「コンプライアンスを確保する」と主張しています。

IT 部門やセキュリティチームは、責任の所在を明らかにする上で適切なチームです。アウトソーシングする必要がある部分と、社内のチームでできる部分の内実を読み解くスキルを持っています。通常、最も価値のある外部ソリューションを最小限の数だけ選択し、最高レベルのセキュリティを確保すると同時に、複雑さを可能な限り軽減することに全力を尽くします。

大規模組織の中には、適用されるすべての法規制に対するコンプライアンスを積極的に達成・維持することを専任とするリソースや「コンプライアンスの専門家」を雇うことを選択するところもありますが、専門チームを雇うための余分な予算がある組織はごくわずかです。

Absolute ができること

コンプライアンスを支援するソリューションの ひとつとして、Absolute Software が挙げられます。Absolute は、コンプライアンスに特化した独立したサービスではありませんが、IT チームとセキュリティチームの双方が、違反につながる問題やインシデントを効果的に排除できるよう支援します。

Absolute は、規制や業界標準によって義務化または推奨されているセキュリティ管理の確立と維持を支援し ます。さらに、ガバナンスと監査に必要な証拠を効率的かつ拡張性の高い方法で提供します。

組織全体にわたるインサイト (洞察) と可視化

リスクベースのコンプライアンス戦略を実現するための最初の、そして最も重要なステップは、組織全体で何が起こっているかを確認することです。エンドポイントによる機密データへのアクセスや保存、安全でないネットワークへの接続、アプリケーションの健全性の低下、重要な脆弱性パッチの適用遅れなどの状況を解決するには、IT 部門とセキュリティ部門の双方がこの情報を把握する必要があります。

Absolute では、管理者は上記のようなあらゆる状況やその他の状況を確認し、評価することができます。管理者は、包括的でカスタマイズ可能なダッシュボードを使用して、組織内のすべてのデバイスのステータスを確認することができます。実際、監査や「コンプライアンス・チェック」を行う場合、このソフトウェアを使用して、すべてのデバイスのセキュリティ状況 (アプリケーションの状態、構成、パッチ適用日などを含む) を示すレポートを即座に作成することができます。

Absolute が提供するインサイトはさまざまな状況で役立ちますが、特にコンプライアンスと強固なセキュ リティ態勢を実現する際に有効です。Absolute プラットフォームを使用すれば、不審な行動、脆弱なアプリケーション、古い OS、設定の逸脱など、すべての事象にフラグを立て、追跡調査することが可能です。このようなリアルタイムの情報により、コンプライアンスとセキュリティの維持が容易になります。

セキュリティ制御のレジリエンスを向上

コンプライアンスの観点からは、洞察力と可視性が重要であるだけでなく、デバイスとアプリケーションの健全性を積極的に維持する能力も不可欠です。

そこで、Absolute Persistence® の出番となります。この技術は、Absolute と世界中の約 30 社のシステムメーカーとの提携により、すでに 6 億台以上のデバイスに搭載されています。一度起動すると非常に回復力が高く、デバイスの再イメージ、ハードディスクの交換、ファームウェアのフラッシュなど、無効化しようとする試みに対抗できる唯一のソリューションです。

これは他の技術では実現できません。

最終的には、Absolut プラットフォームとエンドポイントとの間に安全な常時接続を実現し、これまでにないリアルタイムの可視性、制御、および修復能力を得ることができます。

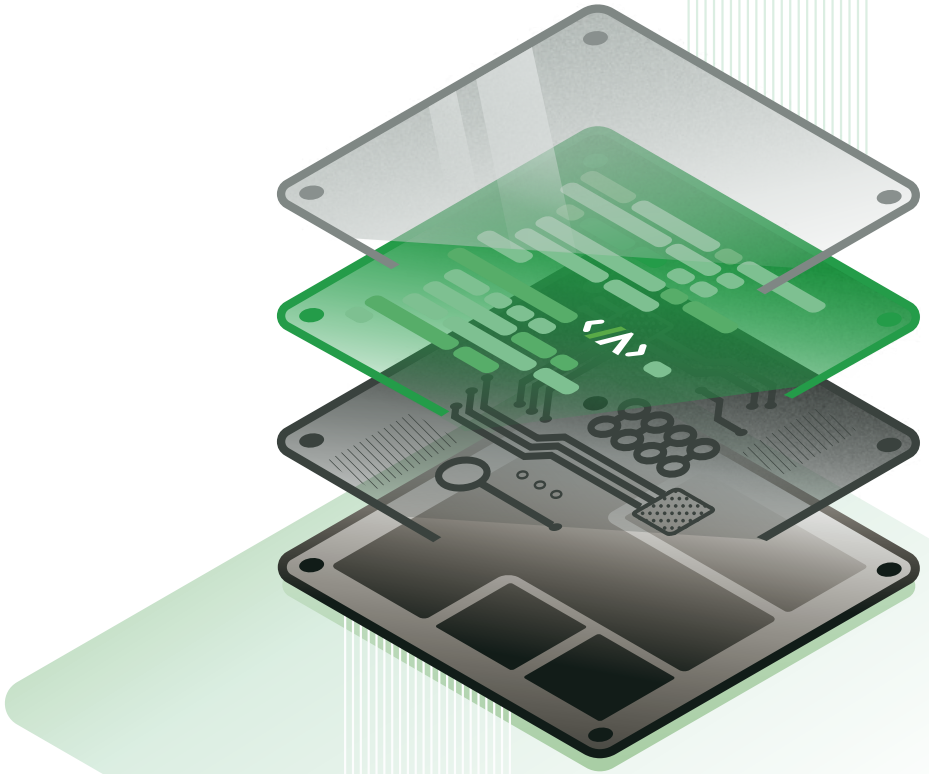
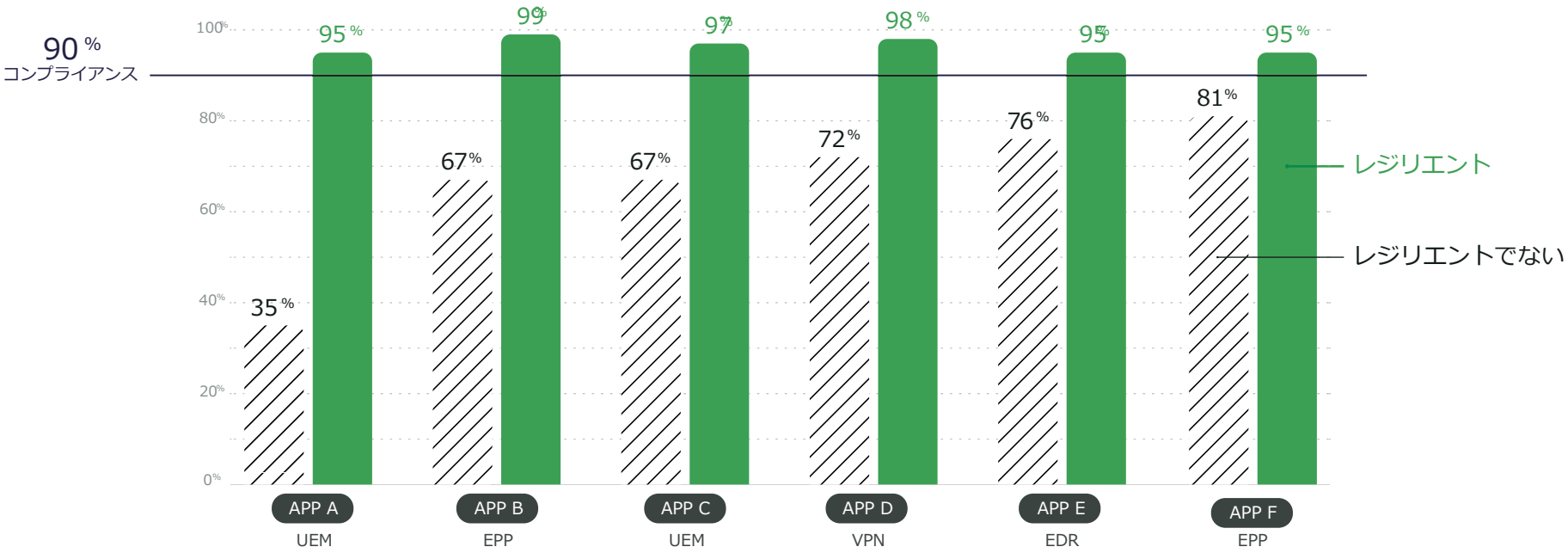


図 1.4
アプリケーションの健全性
レジリエント VS レジリエントでないアプリケーション



2 週間にわたって Application Resilience を有効にしていたデバイス上のアプリケーションは、全体的な健全性を大幅に改善したことが示された。
この分析には、2022 年 8 月 1 日から 2022 年 8 月 14 日までの 100 万台のデバイスで Application Resilience データを持つデバイスが含まれている。
EPP、VPN、EDR、および UEM の各製品カテゴリーに属する 6 つのアプリケーションを分析した。

Absolute プラットフォームは Application Resilience™ を提供し、ミッションクリティカルなアプリケーションの健全性と動作を監視し、欠落、破損、動作不能を検出し、必要に応じてコンポーネントを自動的に修復、再インス トールします (これらを行うために人手を要しません)。Application Resilience は、不健全なアプリケーションを修復することで、セキュリティ管理が期待通りに機能していることを確認し、最適なユーザーエクスペリエンスを提供します (図 1.4 を参照)。

コンプライアンスを監視する IT 部門やセキュリティの専門家にとって、これはどのような意味を持つのでしょうか。

ポリシーの下でアプリケーションの健全性を容易に監視し、その完全性が損なわれていると判断した場合には、自動的にアプリケーションを修復および / または再インストールすることができます。これにより、一般的なソフトウェアの劣化、ソフトウェアの衝突、意図しない削除、悪意のある行為など、何があってもアプリケーションは常に意図したとおりに機能することが保証されます。

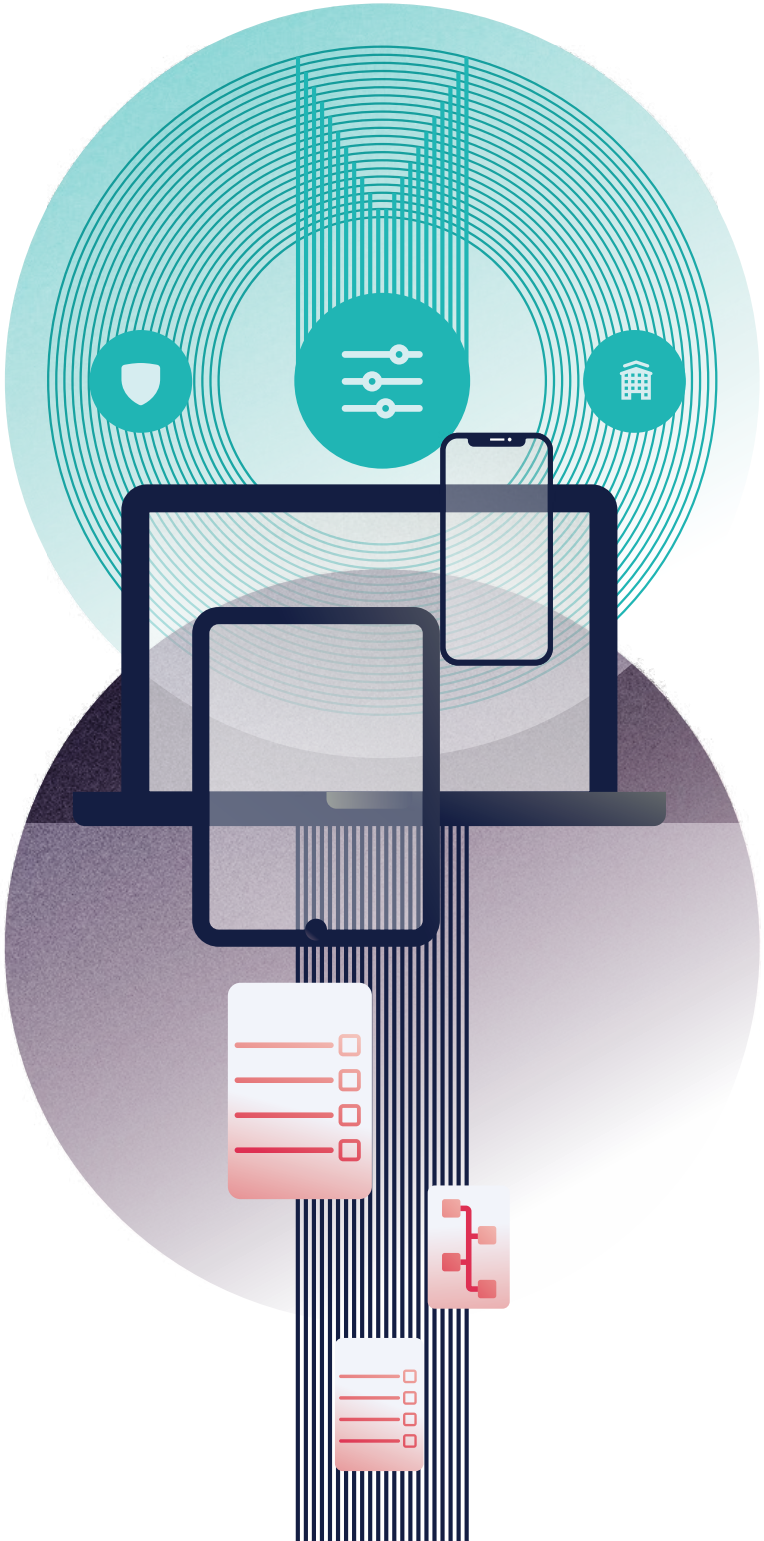
このテクノロジーは、データの保護、つまりコンプライアンスと全体的なセキュリティを確保するためにセキュリティコントロールに依存している組織にとって、大きな負担を軽減することができます。

3. 従来のアプローチを見直し

このレポートから得られる重要な教訓は、コンプライアンスは、扱いづらい時代遅れのテーマではないということです。単に要求事項のリストにチェックを入れるだけでは、組織データを保護し、プライベートに保つという大きな目標を達成することはできません。

真に効果を発揮するためには、コンプライアンスが組織の包括的なセキュリティ戦略の重要な構成要素であり、CISO オフィスによってトップから管理、支援される必要があるのです。

Absolute Software は、リスクベースかつセキュリティに裏打ちされた最新のコンプライアンス戦略を導入する上で、効果的なリソースとなります。詳細については、Absolute までお問い合わせください。



出展

1 https://www.cisa.gov/uscert/ncas/tips/ST04-001
2 https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w
3 https://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf
4 Forrester The 2021 State of Enterprise Breaches
5 Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Gartner, Jan. 2022)
6 https://www.csoonline.com/article/2130877/the-biggest-databreaches-of-the-21st-century.html
7 https://ico.org.uk/about-the-ico/media-centre/news-andblogs/2020/10/ico-fines-marriott-international-inc-184million-forfailing-to-keep-customers-personal-data-secure/

ABSOLUTE®

Absolute Software は、自己復活機能を備えたインテリジェント・セキュリティ・ソリューションを提供する唯一の企業として、2 万社近いお客様に信頼されています。Absolute は、6 億台以上のデバイスに搭載されており、エンドポイント、アプリケーション、ネットワーク接続に可視性、制御、自己修復機能をインテリジェントかつ動的に適用する永久デジタル接続を提供する唯一のプラットフォームで、ランサムウェアや悪質な攻撃の脅威が高まる中、顧客のサイバー耐性の強化を支援しています。

デモやお問合せは
こちら

Nasdaq | ABST

TSX | ABST